AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended)An information security system ~~comprising~~ comprising:

a computer system having security features to prevent its unauthorized use and linked to at least one locking mechanism;

said computer system being configured to be responsive to the presence of an identifiable entity ~~to permit~~ proximate the computer system authorized for ~~accessed~~ access to the computer system ~~and to transmit~~ by transmitting unlocking signals to at least one other linked locking mechanism to cause said locking mechanism to ~~release~~ be maintained in a released state whereby access controlled by said ~~at least one other~~ locking mechanism is specifically permitted while said computer system is ~~VALIDLY accessible~~validly accessed by an authorized user with respect to the computer system's own security features; and

wherein in the event that the computer system enters a state of inhibition of access, the computer system ceases to transmit unlocking signals or transmits a locking signal, so as to cause said linked locking mechanism to enter a locked state unless over-ridden.

2. (Original) An information security system as claimed in claim 1 in which the locking mechanism includes timing means which in the absence of periodic release signals inhibits access after a predetermined time period expires.

3. (Previously Presented) An information security system as claimed in claim 1 in which a plurality of locking mechanisms each controlling access to a respective entity are provided.

4. (Currently Amended) An information security system as claimed in claim 1 in which the ~~or at one of said~~ at least one locking ~~mechanisms~~ mechanism is associated with a respective lockable physical object.

5. (Currently Amended) An information security system as claimed in claim 1 in which the ~~or at one of said~~ at least one locking ~~mechanisms~~ mechanism is associated with a respective electronic or electrical equipment whereby use of such electronic or electrical equipment is only permitted while an ~~authorised~~ authorized user is present.

6. (Currently Amended) An information security system as claimed in claim 1 in association with telecommunications control means arranged to control usage of communication lines whereby telephony or facsimile transmission ~~may be~~ are inhibited in the absence of an appropriately ~~authorised~~ authorized user.

7. (Previously Presented) An information security system as claimed in claim 1 in association with telecommunications control means arranged to control usage of communication lines whereby telephony or facsimile transmission is limited in usage to prevent certain categories of call or communication.

8. (Previously Presented) An information security system as claimed in claim 1 including shared facilities responsive to signals from a plurality of computers each responsive to a respective identifiable entity to permit usage of such shared facilities.

9. (Currently Amended) An information security system as claimed in claim 1 in which ~~the or each~~ said at least one locking mechanism is also responsive to signals from an alternative source to permit access without requiring access to a computer of the system.

10. (Currently Amended) An information security system as claimed in claim 1 in which the locking mechanism is in wired communication with the ~~controlling~~ computer system.

11. (Currently Amended) An information security system as claimed in claim 1 in which the ~~or each controlling~~ computer system includes radio transmission arrangements whereby following ~~authorised~~ authorized access the computer system causes periodic transmission of coded release signals whereby correspondingly coded radio transmission receivers ~~linked~~ provide release instructions to respective linked locking mechanisms.

12. (Original) An information security system as claimed in claim 11 in which the transmission of release signals from a computer may be inhibited if the computer enters a temporary inhibition of access.

13. (Original) An information security system as claimed in claim 12 in which the transmission of release signals is inhibited in the absence of entry of data thereto for a predetermined period.

14. (Previously Presented) An information security system as claimed in claim 1 in association with an environmental control arrangement whereby at least one of lighting, heating and ventilation are controlled in dependence upon the presence or absence of one or more users.

15. (Currently Amended) An information security system as claimed in claim 1 in which at least one ~~of said~~ locking ~~mechanisms~~ mechanism requires the presence of more than one ~~authorised~~ authorized individual.

16. (Currently Amended) An information security system as claimed in claim 1 in which the computer system is linked to a telecommunications system and transmits information defining the identity of the ~~authorised~~ authorized user present whereby associated telephony devices receive facilities and communications appropriate to the respective identified ~~authorised~~ authorized user.

17. (Currently Amended) An office environment ~~comprising~~ comprising:

at least one computer and at least one linked lockable device,

wherein the computer ~~being~~ is responsive to an ~~authorised~~ authorized identifiable entity proximate to the computer system to permit that entity access to use the computer by satisfying security features restricting use of the computer to also effect unlocking of the lockable device ~~to permit~~ thus permitting access to the device while said identifiable entity is ~~present.~~ present and validly authorized to use the computer; and

wherein in the event that the computer enters a state of inhibition of access, the computer ceases to transmit unlocking signals or transmits a locking signal, so as to cause said linked locking device to enter a locked state unless over-ridden

18. (New) A method for providing controlled security over a lock mechanism linked to a computer having security access features which permit only authorized users to have use of the computer, said method comprising:

configuring said computer system to be responsive to the presence of an identifiable entity proximate the computer system and authorized for access to the computer system by transmitting unlocking signals to at least one other linked locking mechanism to cause said locking mechanism to be maintained in a released state whereby access controlled by said locking mechanism is specifically permitted while said computer system is validly accessed by an authorized user with respect to the computer system's own security features; and

in the event that the computer system enters a state of inhibition of access, ceasing to transmit unlocking signals or transmitting a locking signal, so as to cause said linked locking mechanism to enter a locked state unless over-ridden.

19. (New) A method as in claim 18, wherein, in the absence of periodic release signals, access is inhibited after a predetermined time period expires.

20. (New) A method as in claim 18 wherein a plurality of locking mechanisms each control access to a respective item also proximate the authorized entity.